DOD Information Assurance Training & Awareness Products

To order our products, please go to the following website:
http://iase.disa.mil/eta

Web Based Training (WBT)

NOTE: These products are web-deliverable, using html and Flash technology. They can be loaded on web servers for delivery via the Internet or intranet. As with our traditional products, they also run on a LAN or from a CD-ROM drive. A PKI Cert is required for some of the training products.

IA Awareness Training

DoD Information Assurance Awareness (For DoD Personnel)
Date 10/09 – Ver 8.0

Utilizing an interactive format, this web-based product presents topics that reflect the constantly changing world of information assurance as it relates to information technology. The DoD user is introduced to the principles of IA, IA-related laws and policies, and critical infrastructure protection (CIP). The dangers associated with the insider threat, social engineering, and peer-to-peer applications are presented in a clear and understandable format. The course introduces the concept of Malicious Code, including its impacts and the methods it uses to infect information systems. The differences between threats and vulnerabilities are explained and the classification levels for DoD information, to include personally identifiable information (PII) are defined. The role of the DoD user in protecting DoD information and information systems is outlined. The course explains the threats associated with identity theft, spyware, and phishing and how to protect against these threats. Security tips are also provided to practice in the daily work routine as well as at home. (1hr)

Federal Information Systems Security Awareness (For Non-DoD Personnel)
Date 09/09 – Ver 3.0

In this web-based product, the user is introduced to the principles of information systems security (ISS) and its related laws and policies. The importance of critical infrastructure protection (CIP) and the differences between threats and vulnerabilities are explained in a style that reflects the constantly changing world of ISS and its relationship to information technology. Through an interactive format, the user is presented with the dangers associated with the insider threat, social engineering, and peer-to-peer applications. The concept of malicious code, its impact, and the methods it uses to infect information systems are explored. The course identifies important guidelines that define the sensitivity levels of information, including personally identifiable information (PII), and your role as a user in protecting this information. Also explained are the threats associated with identity theft, spyware, and phishing. This course gives information on how you can protect yourself by providing security tips to practice in your daily routine at work and at home on your personal computer. (1 hr)

IC Information Assurance Awareness (For Intelligence Community Personnel)
Date 12/09 – Ver 1.0

This web-based product presents information assurance (IA) for the Intelligence Community (IC) user with a focus on proper classification, marking, and handling of Sensitive Compartmented Information (SCI) within a SCI Facility (SCIF) environment. Precautions in secure SCI custody, transmission, and information sharing are reviewed. The IC user is further introduced to the principles of IA and IA-related laws and policies. The importance of critical infrastructure protection (CIP) and the differences between threats and vulnerabilities are explained in a style that reflects the constantly changing world of IA and its relationship to information technology. Through an interactive format, the user is presented with the dangers associated with the insider threat, social engineering, and peer-to-peer applications. The concept of malicious code, its impact, and the methods it uses to infect information systems are explored. The course identifies important guidelines that define the sensitivity levels of information, including personally identifiable information (PII), and your role as a user in protecting this information. Also explained are the threats associated with identity theft, spyware, and phishing. This course gives information on how you can protect yourself by providing security tips to practice in your daily routine at work and at home on your personal computer. (1.5 hrs)

Using Public Key Infrastructure (PKI)
Date 12/09 – Ver 1.0

This training presents separate PKI Overview and Using PKI Certificates courses, each with its own course completion certificate.

Upon completing the PKI Overview course, Department of Defense (DoD) information systems users will be able to identify what PKI is and why it is important to the DoD, as well as which pieces of Congressional legislation, Federal policy, and DoD guidance mandate the use of PKI. This presentation identifies the different components of PKI and how they are implemented in the DoD. Details discussed include systems, software, PKI credentials, certificates, and keys. DoD users will learn how to use PKI to log on to unclassified DoD networks and access DoD information systems, applications, and websites; as well as how to use PKI to send and receive e-mails securely. Users will understand what the Common Access Card (CAC) is, why they use it, and how and when to obtain or return a CAC. DoD users will be informed on what system elements are needed to use their CAC, to include what a CAC personal identification (PIN) number is and what to do if they forget their CAC PIN. (1 hr)

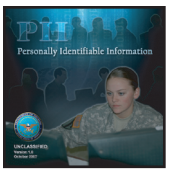
When DoD information system users have completed the Using PKI Certificates course, they will understand how to safely and securely authenticate their identity to access DoD unclassified networks using the PKI certificates contained on their Common Access Card or Alternate Token. DoD users will also learn how to use their PKI certificates to authenticate their identity to DoD systems, applications, and restricted web sites. In addition, DoD users will know how to validate digital signatures, as well as how to send and receive e-mail securely using their PKI certificates to encrypt the e-mail, when necessary. Finally, they will be able to identify how to read an e-mail that was encrypted using expired certificates taken from a previous CAC. (1 hr)

Personal Electronic Devices (PEDs) Removable Storage Media
Date 12/08 – Ver 1.1

In this presentation, Department of Defense (DoD) information systems users will learn about the security risks associated with portable electronic devices (PEDs) and removable storage media. They will learn about the specific security risks associated with these devices, which types of PEDs and removable storage media are of greatest concern to the DoD, and what must be done to mitigate security risks to data stored on these devices. Finally, users will be introduced to DoD policy regarding encryption of data on these devices. (20 min)

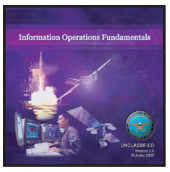
Phishing
Date 04/08 – Ver 1.0

This interactive training explains what phishing is and provides examples of the different types of phishing. It also provides guidelines to help individuals recognize phishing attempts so that appropriate actions may be taken to avoid these attacks and their consequences. It explains that phishing is a serious, high-tech scam and that system users are the best line of defense against phishing. Further, it illustrates why users should always be on the look out for phishing attempts even from people from within their organization. (15 min)



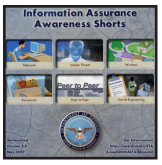
Personally Identifiable Information (PII)
Date 10/07 – Ver 1.0

This web-based training identifies what Personally Identifiable Information (PII) is and why it is important to protect PII. This training reviews a Department of Defense (DoD) organization's responsibilities for safeguarding PII and explains individual responsibilities for PII recognition and protection. Major legal, Federal, and DoD requirements for protecting PII are presented, to include the Privacy Act of 1974, E-Government Act of 2002, and the Federal Information Security Management Act, or FISMA. Federal guidance from the Office of Management and Budget, or OMB, publications is discussed. This training introduces the DoD Privacy Program and reviews PII protection measures mandated by recent Office of the Secretary of Defense memoranda. Significant requirements are reviewed for handling PII and reporting any theft, loss, or compromise of this information. This training is intended for DoD civilians, military members, and contractors using DoD information and information systems. (45 min)



Information Operations (IO) Fundamentals
Date 10/07 – Ver 2.0

IO Fundamentals provides an overview of the military's need for information, how information operations (IO) helps achieve information superiority, and the vital role IO plays in Joint Force operations. This web and computer based (WBT/CBT) course explains what IO is, why it is important, and how IO differs from other DoD activities that involve information. The course also explains the core IO capabilities, the capabilities that support or are related to IO, what an IO cell is, and identifies who is responsible for implementing IO. In addition, this course identifies the key challenges and considerations that must be understood and assessed when planning IO. This product is based on Joint Publication 3-13. (2 hrs)



Information Assurance Awareness Shorts
Date 01/09 – Ver 3.0

This product contains specific information related to the topics listed below.

Insider Threat Short provides awareness about the Insider Threat and the employee behaviors that may signify the potential to be an insider threat. (15 min)

Telework Short introduces the basic concept of telework and covers the fundamental procedures and basic operating guidelines for doing telework from both a government Telework Center and from the home. (15 min)

Wireless Security Short introduces basic concepts in wireless networking security and allows the user to explore the security risks inherent in different network configurations. (15 min)

Passwords Short introduces the importance of complex passwords, including the requirements for creating a password as well as hints for remembering these passwords. (20 min)

Peer-to-Peer Short provides an in-depth treatment of P2P threats and the OMB and DoD guidance on P2P for Department of Defense personnel. (20 min)

Social Engineering Short explains what social engineering is, gives examples of social engineering techniques, describes the possible consequences of social engineering, and provides guidelines to enable the user to recognize and deal with social engineering. (20 min)

IA Training for Senior Leaders

Designated Accrediting Authority (DAA)
Date 03/10 – Ver 7.0

This interactive training provides an understanding of the roles and responsibilities of the DAA. The user will learn about important issues associated with the DAA's responsibilities and the key players that interact with the DAA, including the Principal Accrediting Authority, Chief Information Officer, Certifying Authority, Program Manager, User Representative, Information Assurance Manager (IAM), and Information Assurance Officer (IAO). This presentation also provides legal guidance relating to information system security, to include Congressional legislation, as well as Federal and Department of Defense, or DoD, policy. An overview of DoD certification and accreditation, to include the new DoD Information Assurance Certification and Accreditation Process (DIACAP) and the older DoD Information Technology Security Certification and Accreditation Process (DITSCAP) is also provided. The DAA's responsibilities concerning system connection and in the DoD IA Workforce Improvement Program are reviewed. The information in this product can also benefit mid-level and senior managers. (2.5 hrs)

IA Briefing for Senior Operational Leaders
Date 03/10 – Ver 1.0

The Information Assurance (IA) Briefing for Senior Operational Leaders presents five short scenarios based on problems observed during operations, with the actual or possible consequences that could result from the actions that caused the problems. You, as the senior leader, are challenged to consider how your planning, action, and response could lessen or eliminate these vulnerabilities. (30 min)

DoD Information Assurance Certification Accreditation Process (DIACAP)
Date 01/09 – Ver 1.0

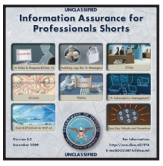
This training presents separate DIACAP Overview and DIACAP Implementation courses.

In the DIACAP Overview course, you will learn that Department of Defense (DoD) information systems, in order to operate, must be certified and accredited, using a standard set of activities defined within the DoD Information Assurance Certification and Accreditation Process, or DIACAP. You will also learn about the DIACAP's purpose, objectives, and implementation, as well as the crucial role that enterprise risk management plays in the certification and accreditation process. DIACAP roles and responsibilities will be explained, to include the DoD enterprise governance structure, DoD Component responsibilities, and DIACAP implementation responsibilities. Further, you will be introduced to the key components of the five DIACAP activities used for DIACAP implementation. Finally, you will learn about transition to the DIACAP from the previous DoD Information Technology Security Certification and Accreditation Process, or DITSCAP. (1 hr)

The DIACAP Implementation course is designed for IA professionals responsible for implementing or involved in supporting activities in different capacities in the certification and accreditation, or C&A, of Department of Defense (DoD) information systems. You will learn about the complete DoD Information Assurance Certification and Accreditation Process, or DIACAP, and how the contents of the DIACAP package are generated. This instruction covers, in detail, the five activities of the DIACAP and the tasks that occur within each DIACAP activity. How to access the tools and resources used to execute DIACAP tasks is illustrated. Finally, the course walks through the roles of the key players involved in implementing the DIACAP activities and tasks that lead to the certification determination and accreditation decision that are needed in order to operate a DoD information system. (1 hr)

Information Assurance Policy & Technology (IAP&T)
Date 03/10 – Ver 5.0

The Information Assurance Policy and Technology (IAP&T) training has been created for Information Assurance Officers (IAOs), Information Assurance Managers (IAMs), and System Administrators (SAs) to aid them in successfully performing their duties in accordance with DoD guidance, pertaining to the defense of DoD information and DoD information systems. Individuals whose duties include IA policy and oversight, inspection and audit, or other functions supporting the Information Assurance mission will find this course useful and meaningful. Depending on your Command, Service, or Agency, the completion of this online course could help the student meet the standards for Level 1 System Administrator certification. This product updates and replaces the IAP&T dated 01/09, version 4.0. (4.5 hrs)

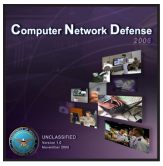


Information Assurance for Professionals Shorts
Date 12/09 – Ver 5.0

This product contains specific information related to the topics listed below.
IA Roles and Responsibilities Short introduces the Information Assurance hierarchy, including the roles and responsibilities of key leadership positions as well as the responsibilities of all Authorized Users. (25 min)
Auditing Logs for IA Managers Short introduces the auditing responsibilities of IA Managers. It describes the audit log and event information displayed by the system's auditing software. (20 min)
Security Technical Implementation Guides (STIGs) Short introduces the purpose and uses of STIGs.
SCADA Short describes how Supervisory Control and Data Acquisition systems function and significant cyber-security issues associated with DoD SCADA systems. (15 min)
FISMA Short explains what the FISMA is, why it is important, how it is implemented within the Federal government and the DoD, and identifies where to obtain guidance for FISMA responsibilities. (20 min)
IA Vulnerability Management Short describes the vulnerability management process in DoD and the tools that support the process. (20 min)
The DoD 8570.01-M IA WIP Short presents an overview of the IA Workforce Improvement Program, defines the DoD IA workforce, and outlines the IA workforce training and certification requirements. (1 hr)
The Zero Day Attack Short provides an introduction to the steps an IA professional needs to follow if they suspect that their system has been compromised by an attack which otherwise is unknown to the IA technical community (aka Zero Day Attack). (20 min)

IA Hot Subjects
Date 11/06 – Ver 1.1

These six short courses are designed for use by individuals who are identified by DoD 8570.01-M, Information Assurance Improvement Program as IAT Levels I and II, as well as IAM Level II. The courses review vulnerabilities which have been around for some time, and which are commonly overlooked in the press of new technology and new threats. These vulnerabilities still provide a foothold for an enemy. Each subject briefly covers the nature of the problem and its general resolution, and is designed to be finished in a half hour or less. The subjects are Transmission Control Protocol (TCP) reset, Distributed Denial of Service (DDoS) attacks on routers, spoofing attacks, remote access/remote control, physical security review, and Simple Network Management Protocol, or SNMP. (1.5 hrs)



Computer Network Defense (CND)
Date 12/06 – Ver 2.0

This product is designed for high-level managers who need to acquire a Computer Network Defense Service Provider (CND SP) for their organization, information assurance (IA) professionals who want to transition into a CND SP career path, and individuals who desire a general knowledge of computer network defense (CND) and CND SPs. This interactive web-based training defines CND, identifies CND requirements for DoD components, key requirements that CND SPs must meet, and the principal services provided by CND SPs. This training presents a high-level explanation of the certification and accreditation (C&A) process for CND SPs. The CND SP principal services are enumerated, to include system protection services, anti-virus, system scanning tools, Information Operations Conditions (INFOCON) Program support, Information Assurance Vulnerability Management (IAVM) support, vulnerability assessment monitoring, analysis, and detection services, as well as incident response. An explanation of the training and future certification requirements for those who work as CND SPs is also included. (1 hr)

Information Assurance/Computer Network Defense Information Sharing
Date 03/10 – Ver 1.0

The Information Assurance (IA)/Computer Network Defense (CND) Information Sharing course is designed to instruct students on the processes and policies involved when attempting to share computer network defense information with coalition partner nations. This course explores the methods and techniques required for implementing an information sharing program. The course defines information sharing and the concept of valuable information. Course material then identifies the types of barriers to effective information sharing, as well as describing approaches to overcoming these barriers. (30 min)

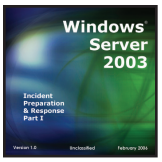
Enhancing Information Assurance through Physical Security
Date 10/07 – Ver 1.0

This interactive course is designed for employees needing a general awareness of how the Department's Information Assurance (IA) program is enhanced through physical security. The course consists of four sections. The first section discusses the discipline of physical security, defines terms, and looks at site selection, physical perimeter, and facility controls. The second section describes some of the threats and vulnerabilities involved in protecting the Department's IA, as well as ways to protect the resources. The third section defines the various types of equipment, and addresses what some of the risks are in using them. The last section introduces policy and best practices for protecting the Department's equipment and information. (2 hrs)

Information Assurance for DoD Auditors and IGs
Date 03/10 – Ver 2.0

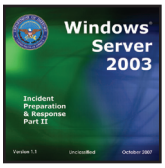
This interactive web-based training introduces the role of the auditor and inspector in information assurance (IA) in the Department of Defense (DoD), to include practical challenges concerning the protection of DoD information systems. This training emphasizes the importance of IA to the DoD's mission, key DoD IA operational roles, and Federal Government, as well as DoD, legal and policy guidance for IA. Use of IA and IA-enabled technology in compliance with the International Common Criteria is detailed. Application of mission assurance category (MAC) and confidentiality level for a DoD information system and enclave is explained. The presentation includes an overview of certification and accreditation of information systems in the DoD, with an amplifying discussion of DoD risk management validation. The basic principles of DoD connection approval processes are addressed. The training concludes with a practical exercise using an audit or inspection of a DoD organization at a forward-deployed location to review the knowledge and IA audit techniques presented. (8 hrs)

IA Technical Training



Windows Server 2003 Incident Preparation & Response (IP&R): Part I
Date 02/06 – Ver 1.0

This course is intended for Information Assurance (IA) Level II Technicians and Managers and for review by Level III Technicians and Managers. Level I IA Technicians and Managers can use the course to prepare for the network responsibilities of Level II positions. Part I of the course focuses primarily on the Information Assurance mechanisms used in Microsoft® Windows® Server 2003. The course describes file systems, some administrative procedures, server management, and folder and file permissions. Topics on security policy, archiving, logs, host- and network-based intrusion detection, as well as third-party tools are provided. A module on Response presents information about preparation, reaction, notification, recovery options, and working with law enforcement. (5 hrs)



Windows Server 2003 Incident Preparation & Response (IP&R): Part II
Date 10/07 – Ver 1.1

This course is designed for individuals who are identified by DoD 8570.01-M, Information Assurance Improvement Program, as IAT or IAM Level II. IAT and IAM Level I personnel who are preparing for the responsibilities of Level II may also find this courseware useful. The course addresses automated check procedures (Gold Disk), checking for IAVM compliance, Windows Active Directory, implementation of IA Policy through checklists and security readiness reviews, and includes an introduction to cyber forensics. (2 hrs)

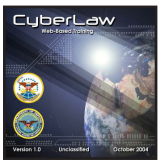
UNIX Security for System Administrators
Date 12/04 – Ver 2.0

This course provides an overview of UNIX security basics for Systems Administrators (SAs) and Information Assurance Officers (IAOs). Topics covered include: network terminology, a framework of UNIX security relating to SA duties, security tools and commands, and reporting mechanisms. The course can be used to provide a conceptual UNIX Security foundation supporting Department of Defense Technical and Management Level I Information Assurance Certifications. It is also appropriate as a refresher for Technical and Management Level II. The course is designed to help beginning to intermediate System Administrators and Information Assurance Officers understand their roles in keeping their system secure; understand vulnerabilities and threats in terms of their origins, methods, and damage capabilities; identify, classify, and use system commands and other tools to assist in keeping the system secure. Because of the wide variety of system configurations, variations among local policies, and rapid technological changes, task specifics are not emphasized in this course. (10.5 hrs)

System Administrator Incident Preparation & Response for UNIX (SAIPR UNIX)
Date 05/05 – Ver 2.01

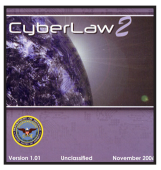
This product was designed to provide Federal System Administrators (SAs) or Information Assurance Officers (IAOs), who have three to five years of experience, with a follow-on course that builds on "UNIX Security for System Administrators, Version 2". It is intended to provide training in preparing for, recognizing, and responding to information systems security incidents from a generic law enforcement perspective. The course touches on computer crimes and laws, system preparation, logs and auditing, mechanics and indicators of intrusion, and the architectures of some common but complex attacks. Updates include more and newer tools to assist the SA, as well as information from newer versions of policies and resources. Biometrics, steganography and other complex techniques are introduced. Intrusion reporting is also discussed. Although some technical aspects of intrusion and malicious code are presented, this is NOT a "hacker's" course. The course supports knowledge needed for Information Assurance Technical and Management Level II, and is appropriate as a refresher at Technical Level III. (6.5 hrs)

CyberLaw



CyberLaw I
Date 10/04 – Ver 1.0

CyberLaw I is a web-based training product for DoD lawyers who need to understand the legal and policy issues, both current and emerging, associated with IA and Critical Infrastructure Protection (CIP.) DoD lawyers will gain an increased ability to recognize and properly analyze legal issues in Cyberspace. The presentation begins with an introduction to the internet. The second module, "Law in Cyberspace," defines computer crime, discusses the First and Fourth Amendments, and presents statutory considerations to be applied during investigations. This module also discusses the four distinct roles or "lanes of the road" pertinent to Computer Network Defense. References are provided throughout the course for lawyers to follow evolving areas of the law in Cyberspace. (6 hrs)



CyberLaw 2
Date 11/06 – Ver 1.01

This product is the second installment in the DoD CyberLaw training suite of products. This course is designed to aid the DoD attorney in keeping abreast of policies and laws that pertain to cybercrime. This course is divided into three sections. The first section discusses issues relating to investigating crime, including the applicability of the Fourth Amendment, honeypots, honeynets, honeygrids, transborder issues, statutory issues, and online undercover operations. The second section addresses issues related to prosecuting crimes and electronic evidence. The third section of this training product addresses post-trial issues and the disposition of evidence. (5.5 hrs)

IA Simulations

CyberProtect
Date 03/10 – Ver 2.0

CyberProtect is a web-based, interactive computer network defensive exercise with a video game look and feel. It is intended to familiarize players with information assurance security terminology, concepts, and policy. Players learn about defensive security tools, which must be judiciously deployed on a simulated network. The player then faces a spectrum of security threats and must make practical decisions for allocating resources (in quarterly increments) using the elements of risk analysis and risk management. Play is divided into four sessions (simulating quarters of a fiscal year). After each session, players receive feedback on how well they are doing. At the end of the last session, players are given a report detailing their cumulative operational readiness rating. The report also details every attack by type, origin, and effectiveness of defensive tools. (2 hrs)

CyberOps:NetWarrior
Date 05/09 – Ver 1.1

CyberOps:NetWarrior is a three-dimensional interactive computer network defense simulation using video game-quality graphics to provide players with an advanced understanding of information assurance (IA) security architecture, terminology, concepts, and policy. Simulation players may create networks using generic hardware, software, and connection tool suites within allocated resource constraints. Players select appropriate generic IA defensive tools for deployment on the networks they have created or on simple, medium, or complex computer-generated networks. Computer-generated attack sequences are used to test the network defenses deployed by exercise players. Simulation play covers IA professional personnel management issues, representing the impact of available IA personnel [system administrators (SAs), information assurance officers (IAOs), and information assurance managers (IAMs)] on the efficiency of system operation. The personnel resource cost of IA professionals can be affected by their training, certification, and experience. CyberOps:NetWarrior is intended to serve as an academic classroom, technical training, and computer network defense exercise support tool. Multiplayer capability permits individual players to assume Blue, Red, and White Team roles in intranet exercise play using realistic exercise architectures. (4 hrs)

CyberOps:NetWarrior was developed from the "Military Academy Attack/Defense Network (MAADNet)" simulation designed by the Department of Electrical Engineering and Computer Science, United States Military Academy. CyberOps:NetWarrior contains advanced elements of the CyberProtect computer network defense exercise.